

EXHIBIT 2

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, <i>et al.</i> ,	:	
	:	
	:	
Plaintiffs,	:	
	:	
v.	:	CIVIL ACTION NO.
	:	1:17-CV-2989-AT
BRAD RAFFENSPERGER, <i>et al.</i> ,	:	
	:	
	:	
Defendants.	:	

ORDER

I.	Introduction	3
II.	Joinder of Municipalities Conducting November 2019 Elections.....	12
III.	Continuing Vulnerability and Unreliability of Georgia’s GEMS/DRE System and Voter Registration System and Database	21
A.	Georgia’s DREs operate on outdated and vulnerable software.....	21
B.	The DREs work in tandem with the Global Election Management System (“GEMS”) interface, which poses additional problems for election integrity and security	25
C.	The DRE/GEMS system is particularly susceptible to manipulation and malfunction.....	33
D.	The State’s expert Dr. Shamos essentially agrees that Georgia’s DRE/GEMS system is not reliably secure.....	42
E.	“What’s Past is Prologue.”	62
F.	The experience of voters in the 2018 election demonstrates serious problems and failures in the State’s DRE/GEMS and ExpressPoll systems.....	90

I. INTRODUCTION

Approximately two months before the 2018 Georgia state general election, this Court recognized in its first preliminary injunction order that the State had “stood by for far too long” in failing to address the “mounting tide of evidence of the inadequacy and security risks” posed by Georgia’s Direct Recording Electronic voting system. *Curling v. Kemp*, 334 F. Supp. 3d 1303, 1307, 1327 (N.D. Ga. 2018). The Court at that time found that Plaintiffs were substantially likely to succeed on the merits of their claims that they faced an imminent threat of the diminishment and burdening of their First and Fourteenth Amendment rights to cast a vote that is properly counted. The Court, however, ultimately determined that the Plaintiffs’ eleventh-hour request for an immediate rollout of paper ballots statewide would likely adversely impact the public interest in an orderly and fair election. But, with the 2020 elections looming around the corner, the Court advised the State Defendants that any new balloting system adopted by the State should address democracy’s critical need for transparent, fair, accurate, and verifiable election processes that guarantee each citizen’s fundamental right to cast an accountable vote. The Court also expressly warned Defendants that further delay by the State in remediating its technologically outdated and vulnerable voting system would be intolerable and any future timeliness objections relating to the State’s inability to comply with the requested relief would be of the State’s own making.

played out with the United States' July 2018 criminal indictment of a host of Russian intelligence agents for conspiracy to hack into the computers of various state and county boards of election and their vendors as well as agents' efforts during the 2016 election to identify election data system vulnerabilities through probing of county election websites in Georgia and two other states.⁷ Similarly, the record demonstrates the perilous vulnerability and unreliability of the State's electronic voter registration system as well as its burdening of Georgia citizens' right to cast a vote that reliably will be counted.

All that said, the posture of the case is also markedly different than in September 2018. The Court concluded in its Order last year that although the Plaintiffs had established a likelihood of prevailing, the balancing of equities and public interest preliminary injunction factors weighed against granting an injunction at that late date because of the magnitude of the administrative and fiscal challenges posed by implementation of a paper ballot system in a statewide election in 2600 precincts and 159 counties. However, the Court forewarned the Defendants that their arguments as to administrative and resource constraints "would hold much less sway in the future" in post-2018 election cycles "if Defendants continue to move in slow motion or take ineffective or no action." *Curling*, 334 F. Supp. 3d at 1327.

⁷ See *United States of America v. Viktor Borisovich Netyksho et al.*, Criminal No. 1:18-cr-215 ¶¶ 69, 75 (D.D.C., July 13, 2018).

On April 2, 2019, the Governor of Georgia approved newly enacted state election legislation.⁸ The legislation replaces the statewide mandated use of DREs with mandated electronic ballot-marking devices (“BMDs”) and optical scanners that count votes recorded on the paper ballots produced via printers attached to the BMDs.⁹ The legislation also revises various voting procedures and provides somewhat vague requirements for expanded auditing of the balloting system and results, using the ballot printout as a key element in the audit process.

The Secretary of State’s Office formally released a request for bid proposals on March 15, 2019, two days after the Georgia Senate approved the legislation. The State represented to the Court that the contract was expected to be awarded by mid-July 2019. Mid-July came and went with no announcement from the State regarding the selection of its voting machine vendor and system. On July 25 and 26, 2019, the Court held a lengthy hearing on Plaintiffs’ renewed injunction motions. The hearing concluded after 8:00 p.m. on Friday evening. First thing Monday morning July 29th, the State awarded the low bidder, Dominion Voting Systems, Inc., the contract for a sum of \$106,842,590.80. The Secretary of State’s contract with Dominion calls for the full implementation of this new voting system in time for Georgia’s March 2020 Presidential Preference

⁸ Georgia Act No. 24, Georgia House Bill 316, amending Chapter 2 of Title 21 of the Official Code of Georgia Annotated.

⁹ See O.C.G.A. §21-2-300. The state additionally authorized up to \$150 million for the contract with a private vendor, to be selected, for purchase of election equipment, software, and services in connection with the new voting equipment and electronic pollbook equipment and supporting software for the electronic voter check-in and verification system at the polls.

Primary as well as a pilot of the system in 6 counties in the November 2019 elections. *See Dominion contract and award documents*, available at <https://sos.ga.gov/securevoting> (last visited August 13, 2019).

The State's response to the current Motions for Preliminary Injunction focused on four themes:

(1) The State contends it has taken substantial proactive, corrective action by passing new election legislation to implement a reliable and secure new election data system based on ballot marking devices, auditable scanned paper ballot printouts, and ballot scanners/tabulators statewide for the 2020 March Presidential Preference Primary.¹⁰ As a result, Defendants further contend that Plaintiffs' request for injunctive relief to bar the use of the DRE system in the 2019 off-cycle elections will cause municipalities and counties to incur significant

¹⁰ The State's contract with Dominion calls for in-precinct scanner/tabulators for the "paper" ballots generated by the Ballot Marking Devices ("BMDs"). The contract also calls for rapid full ballot image/ballot counting scanners for absentee and provisional ballots that are handled in the board of elections office in each county. The printer attached to each BMD used for in-person voting on which the elector electronically marks her vote produces a printed list of the candidates the elector has voted for as opposed to an image of the entire completed ballot as it actually appears on the BMD device screen or if printed on an absentee ballot. The ballot scanner tabulates the selections from each ballot based on the bar code imprinted on the paper printout scanned as opposed to the listing of candidates. The Plaintiffs point out that no elector can visually review and confirm whether the bar code accurately conveys her votes actually cast, as filled out on the BMD screen or appearing on the printout. In other words, a voter cannot verify upon inspection what the bar code on the ballot signifies, *i.e.*, what vote it actually is recording. The State appears to rely on its assessment of the reliability of the equipment software as a whole, the scanner, and the provision of auditing to address this concern. The parties also appear to dispute whether the bar code feature of the new ballot system is consistent with the requirements of the legislation. The State's own expert, Dr. Michael Shamos is not a fan of the type of ballot marking devices chosen by Georgia for its new \$106 million election system that rely on a computer-generated barcode to tabulate the votes, the accuracy of which cannot be verified by the voter. (Shamos Dep. at 56-57.) He agrees that the more reliable approach is the use of a BMD that produces a paper record of the vote tabulation readable by the human voter. (*Id.* at 57.) In any event, this dispute as to the reliability of the bar code voting modality as a transparent, reliable mechanism or its conformity with state law is one not encompassed in the preliminary injunction motions before this Court.

24-28.) As Dr. Halderman¹⁹ testified, the DREs use “a Windows CE operating system that is notoriously insecure. It doesn’t have a security subsystem, for example.” (Tr., Doc. 307 at 137.) The operating system software on Georgia’s DRE machines has not been updated since at least 2005 to address any of the security flaws discovered in the software over the last 13 plus years. (Halderman Decl., Doc. 260-2 ¶¶ 27-28.)

In 2006 Harri Hursti,²⁰ a nationally recognized cyber expert and “ethical hacker,” discovered a serious vulnerability in the AccuVote TSX – the same model of DRE machines used in Georgia. The State Defendants’ own retained expert described this vulnerability in the AccuVote DREs as “one of the most severe security flaws ever discovered in a voting system,” up to that time. (Shamos Dep. at 115.) Hursti’s 2006 security alert report demonstrated numerous vulnerabilities with the AccuVote TSX, the most critical security issue being that the machine’s operating software enables “a malicious person to compromise the equipment even years before actually using the exploit, possibly leaving the voting terminal incurably compromised.... [The] defects compromise the underlying platform and therefore cast a serious question over the integrity of the vote. These exploits can be used to affect the trustworthiness of the system or to selectively disenfranchise groups of voters through denial of service.” Harri

¹⁹ Dr. Halderman’s extensive qualifications as Professor of Computer Science and Engineering and Director of the University of Michigan Center for Computer Security and Society have been previously described.

²⁰ Mr. Hursti has performed several cybersecurity examinations of electronic voting machines of the type used in Georgia.

Hursti, *Diebold TSX Evaluation, Security Alert: May 11, 2006, Critical Security Issues with Diebold TSX*, Executive Summary at 2.²¹

After Hursti's security alert was issued, Diebold was forced to create a security patch for the vulnerable TSX software. There is no evidence that Georgia ever implemented the software patch or made any upgrades to protect the integrity of its DRE machines. (Shamos Dep. 116-17.) Georgia's AccuVote DRE machines use software from at least 2005, which predates the version of the software released by Diebold after the Hursti discovery in 2006 and the updated BallotStation software on the same model Diebold Accuvote TSX machines that were decertified in California in 2006-07 as discussed below. (See Halderman Decl., August 2018, Doc. 260-2 ¶ 25.) Michael Barnes, Director of the Center for Election Systems at the Secretary of State's office, testified that the internal memory of the DRE voting machines themselves has never been tested or inspected by the State. (Tr., Doc. 570 at 77.)

²¹ As Hursti's report explains in greater detail: "Unlike the desktop versions of Windows, the embedded versions of Windows CE 3.x and 4.x versions used in the Diebold system (which are both noncurrent versions) have very limited security features against a user with access below the application level. Because of the lesser security available in Windows CE, access to the standard Windows Explorer application grants users access to replace and modify files almost without restriction. This enables a hostile attacker to severely alter the system functionality and/or add new software (and hidden processes) to the system. In addition to altering individual files, the TSx and TS6 systems also present opportunities to change the Operating System itself. This provides possibilities for hiding the attack and/or altering the application's behavior without any changes to the application itself. A major contributor to this is the ability to change the Operating System functions and libraries any application software relies on at a deep level." (*Id.* at 3-4.)

B. The DREs work in tandem with the Global Election Management System (“GEMS”) interface, which poses additional problems for election integrity and security.

The DREs work in tandem with the Global Election Management System (“GEMS”) – the computer software that generates the ballot programming files.²² (Halderman Decl. ¶ 31) (stating that the computer software that generates the ballot programming files is called an election management system (EMS)). According to Dr. Halderman, “ballot programming files typically are created by election officials either on a regular desktop computer in a government office, or by an election service vendor that creates programming for voting machines across many jurisdictions.” (Halderman Decl. ¶ 31; *see also* Tr., Doc. 570 at 60-61 (Merritt Beaver’s testimony describing the ballot building process and files being moved back and forth from desktop computers to the GEMS server and vice versa).) Michael Barnes, Director of the CES, is responsible for oversight of the GEMS ballot generation files for all 159 Georgia Counties.

The Georgia GEMS server runs on a Windows XP/2000 operating system.²³ (Tr., Doc. 307 at 227, 307-308; Tr., Doc. 570 at 274-75.) In general terms, as explained more fully below, the ballots are constructed in a GEMS

²² A related software program, maintained and licensed by PCC (a different company than ES&S that licenses the GEMS / DRE software), is used to create the ExpressPoll pollbooks providing confidential voter identification information by precinct. Poll workers access this data by computer to verify voter registration and to create the DRE Voter Access Card, which activates the specific electronic ballot on the DRE machine that should be linked to the voter’s address and precinct.

²³ Theresa Payton of Fortalice Solutions, retained by the State to evaluate the security of the Secretary of State’s general computer network system, testified at the 2019 hearing that while software patches are available for the Windows XP operating system, she “wouldn’t want to run [her] stuff on it.” (Tr., Doc. 570 at 275.)

database at the State level, the ballot database is transmitted to the Counties, and then transferred onto memory cards that load the ballots into the DRE voting machines. At the end of the election, the election data from the memory cards is then uploaded onto the County GEMS server that tabulates the county election votes.²⁴ Thus, in addition to serving as the ballot building platform, the GEMS system also serves as a means of communication/transmission of ballot and voting data downloaded to and from the DREs and between the County and State GEMS servers. Because of the interface between the GEMS and the DREs, an infection or intrusion in the GEMS system ballot programming files can spread viruses and malware from the GEMS to all voting machines serviced by GEMS. (See Halderman Decl. ¶ 31.) As described below, a malware or virus attack can occur at any level here (the ballot programming files, DRE removable memory cards, or GEMS database at the County or State level.) (*Id.* at ¶ ¶30-32.)

The testimony of CES Director Michael Barnes about the GEMS system has been inconsistent. At the September 2018 injunction hearing he testified that, “[w]e have an air gapped system within the Secretary of State’s office that holds our ballot-building information, our ballot-building software. And that is the

²⁴ Until the November 2018 election, the SOS allowed county elections offices to transmit their election night results by modem to the state election night server. According to the Election Supervisor for Morgan County, called as a witness by Defendants, the current established state protocol she follows on election night for transmission of County returns instead of the modem transmission is to (1) copy on a flash drive the GEMS election results datafile; (2) take that drive to her internet connected computer; and (3) upload the GEMS vote tabulation results to the Election Night Reporting website run via PCC for the SOS. (Tr., Doc. 571 at 326.) The Georgia State Patrol transports the final CD containing the GEMS database election results from each county back to the SOS some days later, after the County Board of Elections has certified the vote totals.

system that is used to produce that data output.” (Tr., Doc. 307 at 207.) He testified the system containing the “ballot-building software” is never connected to the internet. (*Id.* at 207-208.) He even stated that “[t]he SOS server where the ballot-building information is housed today – I don’t even have access to that server. It is within a locked environment that only the IT systems operators for the Secretary of State’s office have access.” (*Id.* at 208.)²⁵ Barnes testified that the “only thing that is used to transfer data from the private network over to distribution points is a single USB – lockable USB drive . . . used to take PDF files that are generated as proofs to transfer over for county for proofing purposes.” (*Id.* 227-28.) Barnes connects the USB drive to his public internet-facing computer that “is connected to a secure FTP [file transfer protocol] site.” (*Id.* at 228.) But he also stated that the “GEMS server within the Secretary of State’s office that I do my work on does not have a wireless connect point,” which is the basis for his understanding that “it is a secured air gapped system.”²⁶ (*Id.* at 226.)

During the July 2019 hearing, Barnes described the GEMS ballot building process differently than how he portrayed the process in September 2018. The ballots are not built on the private GEMS server in the Secretary of State’s secure facility. (Tr., Doc. 570 at 166-67.) The ballots are built on the GEMS application

²⁵ But he admitted he had no knowledge regarding the security of the software on which the GEMS server operates or “what levels of security they have surrounding that entire system.” (*Id.* at 227.)

²⁶ Merritt Beaver, the Chief Information Officer at the Secretary of State’s Office testified at the 2019 hearing that there is no endpoint protection on the GEMS server because they consider the server air gapped. (Tr., Doc. 570 at 61-62.)

(the “ballot-building software”) on public-facing internet-connected desktop computers of the individual ballot builders, then copied over from the public-facing computer onto a “lockable” USB drive, which is then inserted into the private²⁷ computer to be uploaded into the secure GEMS server for storage of the ballot programming files. (*Id.* at 77-78, 166-67.) Mr. Barnes scans and reformats the lockable USB drive during each transfer. (*Id.* at 77-78, 101, 107.) He follows the same process when copying files from the private GEMS server to the USB drive and back onto the public internet-facing computer for distribution to the counties. (*Id.* at 101, 107.)

The Secretary of State has contracted with ES&S for ballot building support services to “assist” the Center for Election Systems in constructing the GEMS databases that are used within county elections. (*Id.* at 83-84.) Three individuals from ES&S²⁸ work solely on Georgia election databases and perform “their ballot building work within their own purviews” and construct the GEMS databases on desktop computers from their homes. (*Id.* at 84-85.) According to Barnes, the individuals are subject to the same requirements for using air gapped equipment as the Secretary of State, though he testified he does not know what physical security parameters each of the individuals have within their homes. (*Id.* at 85-

²⁷ Mr. Barnes often refers to the private computer housing the GEMS server as “air gapped.” However, as Dr. Halderman and Dr. Shamos both testified – the actual process used by the Secretary of State’s Office does not constitute an “air gapped” system as explained below. The Court will therefore refer to “private” as not being directly connected to the internet.

²⁸ Two of these individuals previously worked for Barnes at CES and the third worked for Cobb County. (Tr. Vol. 1, Doc. 570 at 85.) Barnes was not aware of whether these individuals were employees of ES&S or independent contractors.

86.) These individual contractors built all of the ballots for all counties for the November 2018 general election, and they built the ballots for 98 out of 159 counties for the May 2018 primary election. (*Id.* at 174.)

Once the State collects all of the information from the counties relating to candidates, jurisdictions, and races involved in the election, the three individual contractors construct the initial GEMS databases and initial layout of the data set. (*Id.* at 162.) The databases are then delivered to the SOS on an encrypted CD or locked USB drive. (*Id.* at 163.) Barnes “moves the files from their thumb drives into” the State’s GEMS file system by downloading the data on the public computer and then onto his lockable reformatted USB drive that he “uses for moving the files back and forth” from his public and private/air-gapped computers. (*Id.* at 164-65.) The GEMS server holds the ballot file, which is then placed into a review folder on the server for inspection. (*Id.* at 165.) Barnes and his staff perform a “line-by-line review of the data set to make sure that the right candidates are listed in the right order, names are spelled properly, [and] that the races are in the proper order.” (*Id.* at 163.) If any corrections are needed on the contractor-built GEMS ballot databases, they are not returned to the contractors. Instead, Barnes or his staff make those corrections. (*Id.* at 163-64.)

Barnes described this review/correction process as follows:

A. Once the file is placed into a review folder on the server, then a member of my team – we have a check sheet that is itemized of what we’re looking at that is within a specific database within specific elections. They will then download from the server a copy of that file. And it is saved to their local private CPU. The local – private

CPU is where the GEMS executable application or the GEMS application is residing. The GEMS application is not residing on the server. It is just – the server is just holding files. The GEMS application is on the individual's own CPU. They download a copy of that file onto their computer. They open up the data file on their computer. And they begin examining it to make sure that it has been built properly, that all precincts are there, all district combinations – that all ballots are there, all voting locations. That everything has been built properly.

Q. All right. So then if they make a correction because somebody's name has been spelled incorrectly or for whatever reason, they save it again on that. What happens then?

A. Right. They first – after they have made the correction, the corrected file is residing on their personal CPU. They then create a backup copy of that file and save it back to the server. That saving action back to the server replaces the existing copy with the modified copy. So we only have one copy of the database sitting on the server.

Q. Is that the public server, or is that on your –

A. That is the private.

Q. That is the private, your units?

A. Yes. Everything constructed with the GEMS is done through the private environment.

Q. All right. So then what happens?

A. Then it moves from a review – a review of the database function. Then the file is moved from one folder to another folder. That folder is for audio and visual inspection. Once it is placed into that folder, we have a dedicated room in our office where a member of my team will go in, again copy that file from the server onto a private CPU in order to create an election media, a memory card that is then placed into a touchscreen device within that room. And then we look at the ballot on a DRE to again validate that all the races are appearing, all the candidates are in the proper order, that all the audio files are in place, that we do not see any – any issues with the display of the ballot on the touchscreen. Sometimes because of long questions or such, the screen doesn't look correct in the way it lays things out. So that would make us then make some subtle scaling

adjustments in the display of the database, which requires us to touch the database again.

(*Id.* at 165-67.) This is entirely contrary to the following testimony Mr. Barnes gave to this Court in the September 2018 hearing, just shy of two months prior to the November election:

Q. Do state workers type in every race and candidates' name into the GEMS server?

A. Yes, sir.

Q. So that is how the data gets loaded?

A. Yes, sir. It is all manual entry.

(Tr., Doc. 307 at 226-27.) Despite his testimony in September 2018 that the entire ballot building process is done in-house on a secure GEMS server, the ballot programming was not done by state staff by manual entry directly into the GEMS server housed in the State's secure facility.

Finally, once counties approve the ballot proofs and ballot database reports, CES provides each county with a single CD with a single file that is the County GEMS database. (Tr., Doc. 570 at 170.) The county takes the CD that contains its GEMS database, loads it into their local GEMS computer and creates the various media they use (*i.e.* memory cards) to program and power the DRE and optical scan units. (*Id.*) Election results data from the DRE machines is stored on the memory cards that is transferred back to the County GEMS server for tabulation of results that are subsequently relayed to the Secretary of State both via the Election Night Reporting System and later manual delivery of a CD.

Dr. Halderman was surprised to learn that the Secretary of State's Center for Election Systems uses outside contractors working from their home computers to build Georgia's ballots for use on the DREs. (Tr., Doc. 571 at 87.) These computers that the contractors are working on in their homes are outside the secure facilities that the Secretary of State maintains for ballot building. (*Id.*) The ballot files must be transmitted into the secured facility on USB drives, and the data from those drives is then copied by Mr. Barnes through his public internet-connected computer²⁹ in order to transfer them into the separate/private secure GEMS server. (*Id.*) Thus, the election programming for every county that is programmed by those external contractors, which included every county in Georgia during the November 2018 general election, travelled through an internet-connected computer where there is an attendant risk of infection by malware that can then be spread to voting machines. (*Id.*)

As Dr. Halderman testified, the process that Barnes described using to transfer GEMS files using a "lockable" (presumably a write-protect switch) USB drive is not in fact secure and does not protect the integrity of the GEMS system as portrayed by Mr. Barnes and Mr. Beaver. (*Id.* at 88.) In order to move the files between the USB drive and the computers, Barnes "has to have [the USB] unlocked in his internet-attached computer in order to format it in order to copy files to it." According to Halderman, this process unfortunately exposes the data

²⁹ The public internet-computer screens for standard known malware.

to infiltration by new malware (or other modes of tampering with election software or data) that can then contaminate the entire election system. (*Id.*)

C. The DRE/GEMS system is particularly susceptible to manipulation and malfunction.

In connection with their 2018 preliminary injunction motions, Plaintiffs presented considerable evidence that Georgia's outdated DRE voting system is highly susceptible to manipulation and malfunction. As Plaintiffs' expert, Dr. Alex Halderman testified here (and most recently before the U.S. Senate Select Committee on Intelligence), Georgia's DRES are vulnerable to various routes of infection and attack that are difficult or impossible to detect or reverse. (Halderman Decl., Doc. 260-2.) They include the following: A computer virus could subtly steal votes from one candidate and assign them to another, without detection. A malicious intruder could install malware that would alter the vote count or stop the machine from accepting votes, as demonstrated during the 2018 injunction hearing.³⁰ Anyone with access to a single voter access memory card, could spread malware from the card to DREs and then from DREs to the election management system, potentially infecting the entire voting system. An attacker can access the ballot programming files on an unsecure election management system and piggyback on the pre-election programming process to spread malicious software to the voting machines across all jurisdictions serviced by the GEMS system. And as Dr. Halderman demonstrated in April 2018,

³⁰ There was no means of detection of this as the "malware modified all of the vote records, audit logs, and protective counters stored by the machine, so that even careful forensic examination of the files would find nothing amiss." (Halderman Decl. ¶ 19, Doc. 260-2.)

Diebold DRE machines can be hacked remotely to steal votes, a method by which foreign adversaries could impede elections without any physical access to voting machines. (*Id.* ¶ 26, n. 20.)

Other cybersecurity elections experts have shared in Dr. Halderman's observations of the data manipulation and detection concealment capacity of such malware or viruses, as well as the ability to access the voting system via a variety of entry points. (*See* DeMillo Decl., Doc. 277, Ex. C; *see also* DeMillo Suppl. Decl., Doc. 548 at 75-85 (supplementing his prior expert testimony in connection with 2018 preliminary injunction motion discussed in 2018 Order regarding observation of malfunction of DRE machines and Express Pollbooks during 2018 election);³¹ Buell Decl., Doc. 260-3; Stark Decl., Doc. 296-1; Lamb Decl., Doc. 258-1 at 126-135; *see also* Bernhard Decl., Doc. 258-1 at 33-42.)

³¹ Dr. DeMillo, who also testified at the 2018 hearing, is the Chair of Computer Science at Georgia Tech and Director of the Georgia Tech Center for Information Security, having previously served as the Dean of the College of Computing at Georgia Tech and Chief Technology Officer for Hewlett-Packard. (Doc. 548 at 74.) Dr. DeMillo has conducted research and taught courses relating to voting system and election security since 2002. He helped write guidelines for using electronic voting machines for use by the Carter Center. He also serves on the advisory boards of Verified Voting and the Open Source Election Technology Institute. (*Id.*) Dr. DeMillo is familiar with Georgia's Diebold DRE voting system, its design, the body of academic literature on the system from the last ten years, and its operation as it is deployed in the polling places in Georgia. He is likewise familiar with Georgia's testing procedures conducted prior to machine deployment at the polling places. Dr. DeMillo owns both the Diebold TSx and TS voting machines which he has examined and used to conduct certain experiments related to DRE system security. (*Id.* at 75.) In his November 21, 2018 Declaration, Dr. Richard DeMillo discussed his observations of DRE voting machine and electronic pollbook malfunctions while he served as a statewide pollwatcher during the November 6, 2018 election. (Doc. 548 at 77.) On the afternoon of November 6, 2018, Dr. DeMillo conferred with Harri Hursti (the nationally recognized Diebold voting systems expert that discovered the severely compromised nature of the AccuVote TSX software in 2006 previously mentioned by the Court above) and cyber security researcher Logan Lamb. Hursti and Lamb had just completed a review of technical information at the Anistown voting precinct in Gwinnett County where four-hour voting delays were being attributed to malfunctioning ExpressPollbooks. (*Id.*)

Dr. Halderman and Dr. DeMillo also explained in their testimony in detail the reasons why the DRE auditing and confirmation of results process and parallel testing of DREs used by state officials on a restricted sample basis is of limited value. (Halderman testimony at hearing; Halderman Decl., Doc. 260-2 ¶¶ 35-48; *see also* DeMillo Decl., Doc. 277, Ex. C ¶¶ 10-20.)

This evidence was buttressed by a mounting tide of research and testing by the nation's leading election cybersecurity experts in election cybersecurity. The consensus of these experts, recently reaffirmed by the National Academies of Science, Engineering and Medicine and the U.S. Senate Select Committee on Intelligence reports in September 2018 and July 2019 respectively, has reached national prominence in the general public's understanding of election security. As the Amicus Brief of the Electronic Privacy Information Center discusses, almost from their inception, DREs have been plagued by warnings that the voting machines are unreliable, insecure, unverifiable.³² As the evidence presented by

³² *See, e.g.*, Eric A. Fischer, Cong. Research Serv., RL32139, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues* (2003) (“there appears to be an emerging consensus that in general, current DREs do not adhere sufficiently to currently accepted security principles for computer systems”); David L. Dill, Bruce Schneier & Barbara Simons, Voting and Technology: *Who Gets to Count Your Vote?*, 46 Communications of the ACM 29 (Aug. 2003) (explaining, “[a] computer can easily display one set of votes on the screen for confirmation by the voter while recording entirely different votes in electronic memory, either because of a programming error or a malicious design”); Tadayoshi Kohno, et al., *Analysis of an Electronic Voting System*, 2004 IEEE Symposium on Security and Privacy 27 (2004) (discussing researchers’ findings that DRE software is significantly flawed after the source code for a DRE voting machine was accidentally posted online); Joseph A. Calandrino, et al., *Source Code Review of the Diebold Voting System* 10, Univ. of Cal. (July 20, 2007) (finding the systems of California’s DREs were susceptible to viruses and malicious software, i.e. “malware”); Ariel J. Feldman, J. Alex Halderman, & Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, USENIX/ACCURATE Electronic Voting Technology Workshop (2007) (“[A]nyone who has physical access to a voting machine, or to a memory card that will later be

[A]ll digital information – such as ballot definitions, voter choice records, vote tallies, or voter registration lists – is subject to malicious alteration; there is no technical mechanism currently available that can ensure that a computer application – such as one used to record or count votes – will produce accurate results; testing alone cannot ensure that systems have not been compromised; and any computer system used for elections – such as a voting machine or e-pollbook – can be rendered inoperable.

National Academies of Sciences, Engineering, and Medicine, et al. *Securing the Vote: Protecting American Democracy* 42, 80 (National Academies Press, 2018) (“National Academies Report” or “NAS Report”). The NAS report identified several risks and usability problems with DRE voting machines. (*Id.* at 78.) The advent of DREs in the early 2000s introduced “new technical challenges,” such as touchscreen miscalibration, which causes a voter’s intended selection of one candidate to be misinterpreted as a vote for another candidate. (*Id.*) However, the NAS was even more concerned about the risk of undetectable cyberattacks on DREs that lack a “paper artifact that could be manually counted.” (*Id.*) Furthermore, the NAS report emphasized that any voting system should allow a voter to verify that the recorded ballot reflects his or her intent, which isn’t possible with paperless DRE machines. Although some concerns with DREs are alleviated if the machines create voter verified paper audit trails (VVPATs), the NAS report notes that “it is possible that the information stored in a computer’s memory does not reflect what is printed on the VVPAT.” (*Id.*) The NAS also endorsed the use of “risk-limiting audits,” in which individual randomly selected paper ballots are examined until sufficient statistical assurance is obtained. (*Id.*

at 95.) The key to the NAS recommendation is that paper ballots are required for such audits. The report recommended that voting machines that do not produce paper audit trails “be removed from service as soon as possible” and that “[a]ll local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election.” (*Id.* at 80.)

The NAS report also noted several cybersecurity risks regarding electronic pollbooks and voter registration databases. It detailed concerns about “unauthorized access to or manipulation of the registrant list” because voter registration databases are “often connected, directly or indirectly, to the Internet or state computer networks.” (Doc. 285-1, Ex. 1 at 57.) As an example of the vulnerability of electronic voter databases, the report listed the server error that left 6.5 million voter records in Georgia exposed for six months in 2016-17. (*Id.* at 58.) The NAS report listed a number of ways in which cyberattacks on electronic voter registration data or e-pollbooks could disrupt elections: 1) by altering voter registration databases used to generate pollbooks; 2) by altering the record of which eligible voters have actually voted; and 3) by a “denial-of-service” attack, which would shut down voting altogether. (*Id.* at 72.) Thus, the NAS report recommends that “[j]urisdictions that use electronic pollbooks should have backup plans in place to provide access to current voter registration lists in the event of any disruption.” (*Id.*)

Dr. Halderman most recently testified before the U.S. Senate Select Committee on Intelligence that prominently featured his testimony in its report,

2016 U.S. Election, Vol. 1: Russian Efforts Against Election Infrastructure with Additional Views, 116th Cong., 1st Session (2019) (*partially redacted*) (“SSCI Report”). The Senate Select Committee on Intelligence concurred with the NASEM regarding the susceptibility of electronic voting machines to external manipulation in its report on Russian interference in the 2016 U.S. election.³⁴ Relying on testimony from Dr. Alex Halderman and other experts, the SSCI noted that “researchers have repeatedly demonstrated that it is possible to exploit vulnerabilities in electronic voting machines to alter votes.” (SSCI Report at 40.) A computer virus could steal votes from one candidate and assign them to another or could stop the machine from accepting votes altogether. (*Id.*) According to the Senate Committee report, DRE machines “can be programmed to show one result to the voter while recording a different result in the tabulation.” (*Id.* at 42.) Therefore, the SSCI report called for states to discontinue using DREs, which “are now out of date.” (*Id.*)

The Senate Committee further echoed these findings regarding voter registration systems. After holding hearings, reviewing intelligence, and hearing testimony from state election officials and U.S. Government authorities responsible for election security, the Committee also concluded that voter

³⁴ Report of the Select Committee on Intelligence on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Vol. 1: Russian Efforts Against Election Infrastructure with Additional Views, 116th Cong., 1st Session (2019) (*partially redacted*) (“SSCI Report”). The Senate Select Committee on Intelligence, which was released to the public on July 25, 2019, “sought to determine the extent of Russian activities, identify the response of the U.S. Government at the state, local, and federal level to the threat, and make recommendations on how to better prepare for such threats in the future.” (*Id.* at 3.) The redacted SSCI Report was presented at the July 26th hearing marked as Defendant’s Exhibit 3, but Defendants did not move for its admission into evidence.

registration databases and electronic pollbooks, which can be accessed over the internet, are vulnerable components of U.S. election infrastructure. (SSCI Report at 57.) The July 2019 SSCI report noted that Russian government cyber actors engaged in operations to scan the election-related state infrastructure of all fifty states and conducted research on “general election-related web pages, voter ID information, election system software, and election service companies” and that Russian operatives were able to penetrate the voter registration databases and access voter registration data from Illinois and at least one other state. (*Id.* at 8, 22.)

Counties in Georgia were targeted as well. In July 2018, Special Counsel Robert Mueller released an indictment that alleges that a Russian operative “visited the websites of certain counties in Georgia, Florida, and Iowa” on or about October 28, 2016. (Doc. 471-7 at 3.) As a result, the SSCI report recommends that state officials “[u]pdate software in voter registration systems” and “[c]reate backups, including paper copies, of state voter registration databases.” (SSCI Report at 57.)

D. The State’s expert Dr. Shamos essentially agrees that Georgia’s DRE/GEMS system is not reliably secure.

One might recall that Defendants surprisingly presented no witness with actual computer science engineering and forensic expertise at the 2018 preliminary injunction hearing to address the impact of the breach of the Center for Election Systems servers housed at Kennesaw State University, or the specifics of any forensic evaluation of the servers, DREs, or the State and County

office. In other words, when the Court held its first preliminary injunction hearing in September 2018, the SOS's office had assumed the functions of the CES at KSU ("CES/KSU"), less than a year earlier, on January 1, 2018. (Doc. 472-4 at 2.)

The State Defendants effectively dismiss the significance of the CES/KSU data breach, data systems mismanagement, and record destruction. But as the Court assesses the current operation of Georgia's voting systems and voter registration databases, the legacy of these events stands out.

The Court's September 17, 2018 Order summarized these events as follows:

In August 2016, Logan Lamb, a professional cybersecurity expert in Georgia, went to CES's public website and discovered that he was able to access key election system files, including multiple gigabytes of data and thousands of files with private elector information. The information included electors' driver's license numbers, birth dates, full home addresses, the last four digits of their Social Security numbers, and more. Mr. Lamb was also able to access, for at least 15 counties, the election management databases from the GEMS central tabulator used to create ballot definitions, program memory cards, and tally and store and report all votes. He also was able to access passwords for polling place supervisors to operate the DREs and make administrative corrections to the DREs. Immediately, Mr. Lamb alerted Merle King, the Executive Director overseeing CES, of the system's vulnerabilities. The State did not take any remedial action after Mr. King was alerted.

In February 2017, a cybersecurity colleague of Mr. Lamb's, Chris Grayson, was able to repeat what Mr. Lamb had done earlier and access key election information. Mr. Lamb also found, around this time, that he could still access and download the information as he had before. On March 1, 2017, Mr. Grayson notified a colleague at Kennesaw State University about the system's vulnerabilities, and this led to notification of Mr. King again. Days later, the FBI was alerted and took possession of the CES server.

The Secretary of State has since shut down the CES and moved the central server internally within the Secretary's office. But on July 7, 2017, four days after this lawsuit was originally filed in Fulton Superior Court, all data on the hard drives of the University's "elections.kennesaw.edu" server was destroyed. And on August 9, 2017, less than a day after this action was removed to this Court, all data on the hard drives of a secondary server – which contained similar information to the "elections.kennesaw.edu" server – was also destroyed. As discussed more fully later in this Order, the State offered little more than a one-sentence response to these data system incursions and vulnerabilities at CES.

Curling, 334 F. Supp. 3rd at 1310. The Court further found after hearing Mr. Barnes's testimony at the September 2018 preliminary injunction hearing:

Mr. Barnes professed effectively no knowledge about the ramifications for the state's voter system or remedial measures in connection with Mr. Lamb's accessing the CES's voter registration databases – which was filled with millions of voter records with personally identifiable information, passwords for election day supervisors, and the software used to create ballot definitions, [DRE] memory cards, and vote tabulations.

Id. at 1323.

The Court's closer examination of the record evidence now is even more disturbing. In a detailed email dated August 28, 2016, Mr. Lamb brought to Merle King's attention the CES server exposure and compromise, data exposure, software flaws and security issues – all of major magnitude – that rendered the CES-managed voting system highly vulnerable and subject to dysfunction, erroneous data outputs, manipulation and attack.⁴⁸ (*See generally* Doc. 258-1 at

⁴⁸ Mr. Lamb's affidavit describes the simple scripts that he used to access multiple megabytes of sensitive voter and GEMS data and structural information, that was either publicly accessible or poorly encrypted. He also noted in his email that the Kennesaw server was using Drupal software that is subject to "drupaggedon" malware for which there was a 2014 public advisory,

3. **Issue:** CES confidential data handling processes were not defined ...

(Doc. 1-2 at 99-102.) In other words, critical security issues that Lamb had identified in August 2016 finally caused major alarm bells to go off in 2017 when the University's Information Security Office investigated, independent of CES, following faculty member Andrew Green's communication. But in reality, CES had been advised of these *confirmed* critical vulnerabilities in October 2016 when the KSU Information Security Office had scanned CES's backup Unicoi server and when CES's own staff acknowledged they were merely juggling – but apparently no follow-up had occurred. (*See infra.*)

In late March 2017, KSU began arranging with SOS for the uploading of the CES/KSU Express Poll election files to the SOS server, with some transfer security protocols in place. There is no indication than any measures were taken to address the integrity of the database being transferred given the circumstances.⁵¹ (*Id.* at 191-197.) The accessible files could have been and likely were open to access for far longer than the window of time between Lamb's original review in August 2017 and his second review in March 2017. In his declaration, Mr. Lamb articulated his view as a cybersecurity engineer that “[a]ny malware that may have been introduced during periods of security failure would very likely still be present on ExpressPoll books or on other voting system components which remain in use across the state.” (Doc. 258-1 at 133.) This view

⁵¹ The Court notes, though, that the SOS subsequently purchased new servers for operation of the GEMS system.

as to the danger of contamination was similarly articulated by other cybersecurity experts in this case, including the State's expert and consultant, Ms. Theresa Payton.

The Court well understands the challenges every state faces in running elections in this era. But the State Defendants' insistence that nothing amiss happened in the gaping breach and exposure of the CES/KSU electronic election management system and voter databases contradicts the evidence. Similarly, Defendants' blithe blindness to the potential reverberations that would follow the GEMS system and voter registration databases upon transfer to the SOS, after such an exposure and system management, contradicts the fulsome expert opinion and evidence provided in this case.

CES's executive staff were in the loop in all communications regarding the servers supporting the CES's operations, transfer of the election and data systems to the SOS, Open Records Act requests, and requisite records retention. And they were engaged as well when KSU retrieved and wiped the servers in the months after the FBI made forensic images of the servers.

Given the entire course of events described here, the Defendants' contention that the servers were simply "repurposed" and not intentionally destroyed or wiped is flatly not credible.⁵² (State Defs.' Resp., Doc. 558 at 2, 11 -

⁵² In stating this, the Court observes that it has carefully reviewed the parties' briefs and additional attached evidence as to spoliation issues. The notion, argued by Defendants, that Lamb's exposure of the software flaws and data system exposure was not front and center in the original state lawsuit (later removed to this Court) is far-fetched. (*See* Doc. 1-2, ¶¶ 1-36, 93-95, 98) (recounting the entire set of episodes involving the software defects and data breach and

14.) This is especially so given the sensitivity of these circumstances, state record retention requirements, and the correlation of the server destruction or erasures with the filing of litigation and removal of the case to the federal court.⁵³ Simply put, without reaching the issue of spoliation and presumptions or consequences, the Court seriously views the evidentiary import of the Defendants' handling of the servers and its connection to assessing other record evidence – and this course of conduct casts a disturbing shadow on Defendants' posture here.⁵⁴

Similarly, Defendants' denial and dodging before the Court regarding the known veracity of Logan Lamb's proactive alerts to CES/KSU as to the broadscale vulnerability of its election servers, software, and databases both undermines the credibility of Defendants' representations and signals the election system

vulnerabilities identified by Lamb and his colleagues and relying on such in Plaintiffs' claims that Defendants had run the congressional election on an insecure, unsafe, and compromised election data system, inclusive of defective DRE voting machines); *see also*, Count II claim pursuant to 42 U.S.C. § 1983.) Service of the July 3, 2017 lawsuit was provided prior to the server destruction and news of the filing of the suit appeared soon after its filing.

⁵³ The Coalition Plaintiffs did not file a spoliation sanctions motion but instead requested that the Court view the evidence through the lens of spoliation legal doctrine and presumptions in a hearing brief filed on July 25, 2019. And in that connection, the Coalition Plaintiffs ask the Court also to consider other evidence regarding Defendants' alleged mis-handling and failure to preserve DRE machines and memory cards that were subject to litigation holds and preservation obligations. The Court was actively involved in assisting the parties in addressing voting equipment preservation agreements that both preserved voting equipment evidence for later inspection and trial and allowed flexible arrangements to assure that no county would lack sufficient equipment for running elections. Given the extended period when discovery in this case was stayed due to Defendants' motions to dismiss and appeal and that Plaintiffs only filed their spoliation brief during the most recent injunction hearing, the Court will not endeavor to parse out at this point all that may well have gone wrong in preservation of the DRE machines and cards.

⁵⁴ The Court cannot fathom why Defendants' prior counsel did not proceed with their representation to Plaintiffs' counsel in their October 26, 2018 notice of intent to subpoena the FBI's CES/KSU server images for evidentiary preservation purposes. Fortunately, despite the notice's statement that the FBI would otherwise destroy the image because the FBI's KSU investigation was now closed, that apparently has now turned out to be incorrect. The FBI has now indicated the server images remain available and will make arrangements for their production. What data was left on the servers imaged, however, remains a question.

The above findings coincide with and support the validity of the broad range of voter complaints in 2017 and 2018 regarding the inaccuracy and jumbled status of the voter registration records that burdened or deprived them of their voting rights, discussed later in this Order.

The SOS did not ask Fortalice to look again at the issues flagged regarding PCC's aged software, voter database and voting data security issues in the February 2018 report or to follow-up on whether PCC had implemented any of its recommendations. (Tr. Vol. 1, Doc. 580 at p. 40.) Indeed, in his testimony at the July 25, 2019 hearing, Mr. Beaver, the CIO of SOS, could not recall any of the identified issues or recommendations in the February 2018 report until he was furnished a copy of the report to review. The SOS – and its staff – have consistently previously maintained before this Court that there are no problems with the voter registration data system and database that generate the ExpressPoll electronic report that is the gateway for voters at the polls. Further, the SOS, which was in exclusive control of the Fortalice/Cloudburst Report information regarding the system's exposure of the voter registration database and its severe vulnerability at the time of the September 2018 preliminary injunction hearing, never disclosed any form of this information, even though the integrity of the voter database was squarely at issue then. (Testimony of Merritt Beaver, Tr. Vol. 1. at 65-67.) In this same vein, Defendants contended that Logan Lamb's ability to access through the KSU CES server multiple gigabytes of voter

be incorrectly advised that she is not eligible to vote at all, as opposed to being eligible to cast a vote in that precinct using a provisional ballot. (PX 16, Doc. 565-16 at 4.)

registration data from CES databases filled with the personal identifying information of millions of Georgia voters as well as county and state election staff passwords⁶⁵ was not of real significance. The evidence clearly indicates to the contrary.

Fortalice's November 2018 assessment (its third and last report) returned again to focus on the "walls of the castle" of SOS as a whole. It found that SOS had fully remediated just three of the 22 deficits identified in October 2017. (PX 3, Doc. 561-3.) While noting the SOS's progress, Fortalice made twenty additional cybersecurity recommendations to protect the confidentiality, availability, and integrity of voting and voter data for the citizens of Georgia, fourteen of which were of low to no cost. And it identified the ten top cybersecurity risks from 2017 that carried over through 2018, three of which fell outside the scope of the 2018 assessment requested and were deemed unresolved. (The unresolved, out of scope, risks included: insufficient firewall protection for a SOS server; external website vulnerabilities; and "identity and access management controls and voter information privacy controls lacking on PCC's eNet system which houses Georgia's Voter Registration Database.") (*Id.* at 8-9.)

⁶⁵ In his August 3, 2018 declaration, Mr. Lamb additionally makes clear the implications of the loose accessibility of passwords for election day supervisors. "Supervisor passwords control the administration of the DRE voting machines in the polling place including opening and closing of the voting machines as well as making administrative corrections when problems are encountered." (Doc. 258-1 at 130.) He also notes that the ExpressPoll units' files can be modified when voters are checked in to vote, so as to change the voter's assigned "ballot style" (i.e. ballots differ depending on the electoral races listed) and impact whether the voter is approved for voting at the specified polling place. (*Id.* at 130-131.)

The Court will not delve into the details of the Fortalice system penetration efforts, because as Fortalice notes, the SOS limited the time frame allotted for external testing and an external hacker would not necessarily operate with such a time limit but would persist in attempts to obtain access. Fortalice therefore assumed the person or entity had breached the security wall and tested the scope of what the “attacker” could gain access to or control on the network if initial penetration was made. Once again, Fortalice was able through its probing to ultimately compromise accounts and gain access and control the domain administrator over the system.⁶⁶ “During the course of the assessment, Fortalice identified large repositories of voter registration information on network file shares accessible to all domain users” which pose security management challenges. (*Id.* at 29.) Its search of all network locations “was not exhaustive and additional review should be performed by SOS GA IT staff in order to identify all instances of sensitive data stored insecurely.” (PX 3, Doc 561-2 at 19, 29.) At the July 25, 2019 hearing, Mr. Beaver affirmed that this related to PCC’s management of the database and therefore that no more SOS follow-up would have been done. (Tr. Vol. 1., Doc. 570 at 69.) But this Fortalice finding was made in connection with SOS’s storage of sensitive information hosted on file shares on its server(s) accessible to all domain users on the SOS system. (PX 3, Doc 561-2 at 19, 29.) In any event, Mr. Beaver testified that there were no updated reports conducted assessing this exposure of voter registration information on the SOS

⁶⁶ To assure SOS system security, the Court here will not discuss in greater detail Fortalice’s methods or findings in connection with this 2018 penetration testing.

consequences. Mr. Beaver's view neglects to consider that any cyber intruder's scraping of voter personal information from the My Voter Page website could easily be used in other nefarious ways in the election process. Indeed, this concern clearly was identified in warnings provided by the FBI and the Department of Homeland Security as well as in the United States' 2018 indictment of multiple Russian agents.

Most recently, on July 1, 2019, the SOS assumed operational responsibility for hosting the SOS/PCC Technology database. However, the Secretary of State has continued to contract with PCC to maintain its software application for which needed patches are not available and which Fortalice viewed as critically vulnerable. It is unclear, given the history here as well as the SOS's new contract with Dominion, what this change actually encompasses. The voter registration database, containing millions of Georgia voters' personal identifying information, plays a vital role in the proper functioning of the voting system. Yet it has been open to access, alteration, and likely some degree of virus and malware infection for years, whether in connection with: CES/KSU's handling of the system and data and failure to address these circumstances upon transfer of CES's functions back to the SOS; failure to remediate the database, software and data system flaws and deficiencies; or exposure of the widespread access to passwords to the voter registration data system throughout the SOS, CES/KSU, the 159 counties, or the public via the virtual open portal maintained at CES/KSU. Most significantly, the programming and use of ballots in both the DRE and future

Dominion BMD system is tied to the accuracy of voter precinct and address information. Inaccuracy in this voter information thus triggers obstacles in the voting process. New Dominion express poll machines bought as part of the new contract with Dominion cannot alone cleanse the voter database to be transferred and relied upon.

In sum, the Court recognizes that the Secretary of State's Office and its leadership have likely benefited from the information provided in the Fortalice evaluations. Hopefully, this information translates into true intervention. All told, though, the picture remains that in the current cyber environment, the *present* voting system and voter registration database and system, as constituted and administered by the SOS and counties, bear critical deficiencies and risks that impact the reliability and integrity of the voting system process. The transference of defective voter data from one express poll electronic gateway to another one (whether or not the software is PCC's or Dominion's) remains a formidable obstacle to essential change of the voting system.⁷⁰ If voters' capacity to cast votes

⁷⁰ The State's contract with Dominion provides that "Dominion's Democracy Suite Election Management System shall have the capability of importing election data from the State of Georgia's current database to generate ballot layout used to conduct an election." (Contract, Ex. B, § 10.8 at p. 61.) According to the State's filing in response to this Court's inquiry, "the database referred to in Section 10.8 is the voter registration database," which "creates a flat, delimited text export file that contains no executable code and includes precinct and ballot combo information for import into [Dominion's] EMS." (Doc. 556 at 3.) The State's RFP provides that the vendor's new EPoll Data Management System must have the following capabilities: (i) being "[u]sed to combine voter registration and election ballot data into an election-specific elector's list that power the electronic poll book (EPoll) and provides each voter with the properly assigned ballot style;" and (ii) "[a]ccept[ing] imports of voter registration data from eNet on removable memory devices for the purposes of building an elector's list for any given election. The data transferred from eNet includes but is not limited to: voter name, voter address, driver's license number, voter registration ID, voter status, assigned precinct, assigned district combination value, assigned polling place, polling place address, [and] absentee status."

accurately will be counted or counted on the same basis as someone using another voting method. Plaintiffs have shown that the corrosion of the accuracy and reliability of the mandated electronic voter registration database and Express Poll system used at the polls in tandem with the DRE/GEMS voting system has seriously aggravated the arbitrary and unlawful character of Defendants' implementation of the State mandated voting system, in derogation of their First and Fourteenth Amendment rights. Plaintiffs have also shown the imminent risk of harm in the burdening or deprivation of these rights in the upcoming 2019 elections.

When deciding whether state-enacted election methods and procedures violate the Fourteenth Amendment, the Court must weigh the character and magnitude of the burden the State's rule imposes on those rights against the interests the State contends justify that burden and consider the extent to which the State's concerns make the burden necessary. *Timmons v. Twin Cities Area New Party*, 520 U.S. 351, 358 (1997); *Burdick v. Takushi*, 504 U.S. 428, 434 (1992) ("The Constitution provides that States may prescribe '[t]he Times, Places and Manner of holding Elections for Senators and Representatives,' Art. I, § 4, cl. 1, and the Court therefore has recognized that States retain the power to regulate their own elections."); *Anderson v. Celebrezze*, 460 U.S. 780, 788 (1983) ("Although these rights of voters are fundamental, not all," state election laws, "impose constitutionally-suspect burdens on voters' rights . . ."). Because the right to vote is fundamental and the exercise of that right "in a free and

unimpaired manner is preservative of other basic civil rights, any alleged infringement of the right of citizens to vote must be carefully and meticulously scrutinized.” *Reynolds*, 377 U.S. at 562; *Democratic Executive Committee of Florida v. Lee*, 915 F.3d at 1319 (noting that the Supreme Court has “long recognized that burdens on voters implicate fundamental First and Fourteenth Amendment rights”).

The Fourteenth Amendment due process clause protects against “the disenfranchisement of a state electorate.” *Duncan*, 657 F.2d at 708. “When an election process ‘reaches the point of patent and fundamental unfairness,’ there is a due process violation.” *Florida State Conference of N.A.A.C.P. v. Browning*, 522 F.3d 1153, 1183–84 (11th Cir. 2008) (quoting *Roe v. Alabama*, 43 F.3d 574, 580 (11th Cir.1995) (citing *Curry v. Baker*, 802 F.2d 1302, 1315 (11th Cir.1986))). And “[w]hen a state adopts an electoral system, the Equal Protection Clause of the Fourteenth Amendment guarantees qualified voters a substantive right to participate equally with other qualified voters in the electoral process.” *Reynolds*, 377 U.S. at 566; *see also Harper v. Va. Bd. of Elections*, 383 U.S. 663, 665 (1966). In any state-adopted electoral scheme,

[t]he right to vote is protected in more than the initial allocation of the franchise. Equal protection applies as well to the manner of its exercise. Having once granted the right to vote on equal terms, the State may not, by later arbitrary and disparate treatment, value one person’s vote over that of another.

Bush v. Gore, 531 U.S. at 104–05; *see also Davis v. Bandemer*, 478 U.S. 109, 124 (1986) (noting that “everyone [has] the right to vote and to have his vote

Based on its current plan of a progressively-phased rollout by county, the State must have a backup plan ready to be put in place because the risk inherent in the aggressive implementation schedule and the State's own demonstrated functionality issues may compromise the schedule. In opposing Plaintiff's motion, the State argued it did not wish to be put in the position of jeopardizing and testing the organizational capacity of its elections personnel to properly run an election because of any remedy required by the Court. The State must take sufficient and necessary action so that it does not put itself in that same position in the March 2020 Presidential Primary election and beyond – by leaving some portion of the State's voters in the position of being forced to use the current defective voting system as the default voting fallback. Continued use of the GEMS/DRE system past this 2019 cycle of elections is indefensible given the operational and constitutional issues at stake.

With the scanning technology provided by Dominion under the State's contract and funds authorized in connection with HB 316, the State has available to it an acceptable default backup voting option. It is far more logical, efficient, and feasible to use the paper ballot scanning features of the State's newly adopted system as a compliment and default backup, rather than using the DRE/GEMS system, in the event problems with full implementation of the BMDs occur. And it is consistent with the ultimate objective and statutory scheme of the voter verifiable BMD system than the non-auditable, non-voter verifiable DRE system. To the extent there are administrative or fiscal issues arising from any need to

acquire additional or different scanners from Dominion to enable a default option – if required – the Court notes that: (1) Dominion’s RFP and contract documents clearly indicate its ready capacity to deliver additional scanners on a timely basis upon request; and (2) the Legislature authorized the expenditure of up to \$150 million for the implementation of a new voting system – the Dominion contract came in at approximately \$106 million. By contrast, if used as a fallback, the GEMS/DRE system would require a new round of ballot programming and building, separate from the new BMD ballot building – and it would require continued servicing and use of the DRE machines as well as coordination with the Secretary of State elections staff, just to start with.

Under the contract with Dominion, Georgia should have purchased the necessary paper ballots, optical scanners, and HAVA-compliant ballot marking devices for at least six counties for use in the November 2019 elections. The contract further requires that the State and Dominion will have completed training on the new procedures, systems, and equipment, and training protocols for the six pilot counties by the time of the November 2019 election.

Based on the legal posture of this case and constitutional relief issues at stake, the BMD rollout circumstances described above, the essential need for the Secretary of State’s Office to plan for a default backup option in the event of incomplete rollout of the new BMD system for the March 2020 elections (other than use of the GEMS/DRE system in full or part), the State Defendants are **DIRECTED:**

- (1) To refrain from the use of the GEMS/DRE system in conducting elections after 2019.
- (2) To develop a default plan for use in the 2020 elections that addresses the contingency that the new BMD system enacted by the State Legislature may not be completely rolled out and ready for operation in time for the March 2020 Presidential Primary elections or in subsequent elections in 2020 and provide, as part of that contingency plan, for the use of hand-marked paper ballots for voting, in coordination with scanners and other equipment available through the State's contract with Dominion or amendment of such. To assist in the development of this contingency plan, the State Defendants shall identify a select number of counties or jurisdictions that agree to implement a pilot election in November 2019 using hand-marked paper ballots along with optical ballot scanners and voter-verifiable, auditable ballot records.¹⁰⁰ State resources (i.e., appropriate optical ballot scanners, voting booths, ballot supplies, and training materials, as needed) shall be made available for implementation of the pilot.
- (3) File with this Court a copy of any proposed Rules as well as Final Rules adopted by the Georgia Board of Elections or the Office of the

¹⁰⁰ Counties or jurisdictions where one or more municipalities are already using hand-marked paper ballots or other jurisdictions that have had experience with hand-marked paper ballot voting in the past may provide the easiest viable candidates at this juncture.

Secretary of State relating to protocols and provisions for the auditing of election results and ballots, as authorized or required under O.C.G.A. § 21-2-498 as amended, within two days of their issuance. *See also* O.C.G.A. §§ 50-13-4 and 50-13-7.

Plaintiffs additionally request injunctive relief relating to the voter registration database that the Defendants use as the foundation of the ExpressPoll system. Thus, as a matter of security of the voting process and ExpressPoll system tied to the casting of ballots, and to address on a narrowly tailored basis the voter database problems extensively identified here that present an imminent threat to voters' exercise of their right to vote,¹⁰¹ the Court **DIRECTS:**

1. The State Defendants to develop a plan for implementation **NO LATER THAN JANUARY 3, 2020**, that addresses the procedures to be undertaken by election officials to address errors and discrepancies in the voter registration database that may cause eligible voters to (i) not appear as eligible voters in the electronic pollbooks, (ii) receive the wrong ballot, (iii) be assigned to the wrong precinct in the electronic pollbook, or (iv) be prevented from casting a regular ballot in their

¹⁰¹ This injunctive relief is consistent with the findings of the National Academies of Science Report detailing the various methods in which contamination of voter registration data and electronic pollbooks used in conjunction with voting systems disrupts elections and its recommendation that all jurisdictions using electronic pollbooks "should have backup plans in place to provide access to current voter registration lists in the event of any disruption." (NAS Report at 72.)

properly assigned precinct. A copy of the plan shall be provided to Plaintiffs' counsel.

2. The State Defendants should require all County Election Offices to furnish each precinct location with at least one printout of the voter registration list for that precinct.
3. The State Defendants should provide clear pre-election guidance to all County Election Offices regarding all polling officials' mandatory duty under law to provide voters the option of completing provisional ballots, including those who do not appear on the electronic voter registration database at a specific precinct or at all.
4. The State Defendants should continue in future elections to prominently post information concerning the casting of provisional ballots and voters' submission of additional information, including their registration status, and voters' capacity to check the status of their provisional ballot on the SOS website throughout the course of any state or federal elections.
5. The Secretary of State's Office should work with its consulting cybersecurity firm to conduct an in-depth review and formal assessment of the issues relating to exposure and accuracy of the voter registration database discussed here as well as those related issues that will migrate over to the State's database or its new vendor's handling of the EPoll voter database and function.

VI. CONCLUSION

The Plaintiffs' voting claims go to the heart of a functioning democracy. As the Court commented in its Order last year, "[a] wound or reasonably threatened wound to the integrity of a state's election system carries grave consequences beyond the results in any specific election, as it pierces citizens' confidence in the electoral system and the value of voting." *Curling*, 334 F. Supp. 3d at 1328. The reality and public significance of the wounds here should be evident – and were last year as well.

The long and twisting saga of Georgia's non-auditable DRE/GEMS voting system – running on software of almost two decades vintage with well-known flaws and vulnerabilities and limited cybersecurity – is finally headed towards its conclusion. The new Georgia electronic BMD voting system legislation adopted in 2019 was accompanied by a major funding appropriation. The legislation is an essential step forward out of the quagmire, even if just to terminate use of an antiquated vulnerable voting system, with funding for a replacement voting system and the initiation of some measure of future ballot audit protocols. The wisdom or legal conformity of the Secretary of State's selection of a new vendor's particular ballot system though is not the question now before the Court.¹⁰²

¹⁰² As discussed at length in this Order, the premier 2018 Report of the National Academies of Sciences, Engineering, and Medicine recommends the use of paper ballots based on its finding that "[c]omplicated and technology-dependent voting systems increase the risk of (and opportunity for) malicious manipulation." (NAS Report, Doc. 285-1 at 128.)

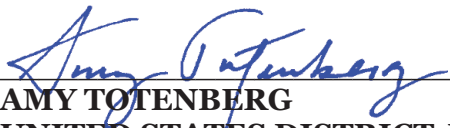
The past may here be prologue anew – it may be “*like déjà vu all over again.*”¹⁰³ The Defendants have previously minimized, erased, or dodged the issues underlying this case. Thus, the Court has made sure that the past is recounted frankly in this Order, to ensure transparency for the future.

For the reasons discussed at length in this decision, the Court **GRANTS IN PART** and **DENIES IN PART** Plaintiffs’ Motions for Preliminary Injunction [Docs. 387 and 419]. The Court **DENIES** Plaintiffs’ request to enjoin the use of the GEMS/DRE system in the 2019 elections, but it **GRANTS** Plaintiffs’ motion to the extent that the Court **PROHIBITS** any use of the GEMS/DRE system after 2019. The Court grants additional measures of relief, as described at the conclusion of Section V above. The Court specifically grants narrowly tailored relief measures to ensure that the GEMS/DRE system is not resorted to as a stopgap default system in the event the Secretary of State and its contractor are unable to fully and properly rollout the new BMD system in time for the 2020 Presidential Preference Primary or any of the ensuing elections. And it requires that the State Defendants promptly file with the Court all proposed and final audit requirements that the State Elections Board and Secretary of State’s Office considers or approves in connection with elections to be held in 2020 or thereafter. Finally, the Court views the significant voter registration database and related ExpressPoll deficiencies and vulnerabilities demonstrated in this case as a major concern both relative to burdening or depriving voters’ ability to

¹⁰³ Quotation attributed to Yogi Berra.

actually cast ballots. The Court therefore requires the State Defendants to develop procedures and take other actions to address the significant deficiencies in the voter registration database and the implementation of the ExpressPoll system.

IT IS SO ORDERED this 15th day of August, 2019.



AMY TOTENBERG
UNITED STATES DISTRICT JUDGE